BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04K 1/00, H04L 9/00

A1

(11) International Publication Number: WO 98/40982

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/US98/04606

(22) International Filing Date: 10 March 1998 (10.03.98)

(30) Priority Data:
60/040,958 12 March 1997 (12.03.97) US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US 60/040,958 (CIP)
Filed on 12 March 1997 (12.03.97)

(71) Applicant *(for all designated States except US)*: VISA INTERNATIONAL [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US).

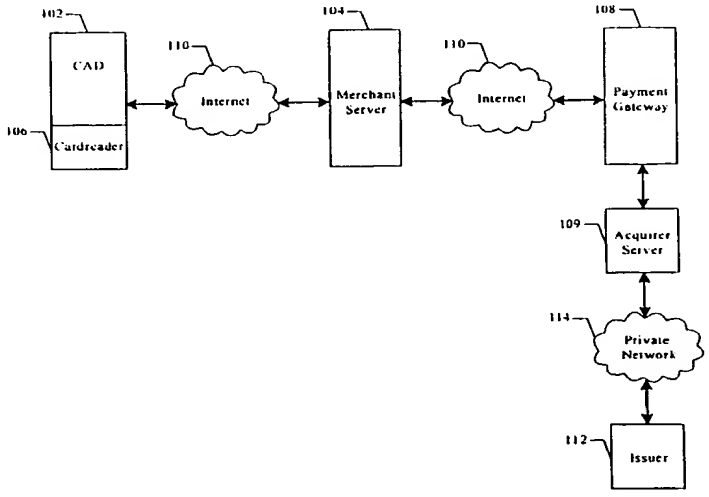
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: KEATHLEY, Kimberly, Ann [US/US]; 18552 Center Street, Castro Valley, CA 94546 (US). CHEN, Ann–Pin [US/US]; 600 Somerset Lane, Foster City, CA 94404 (US). MCCUSKER, Nancy [US/US]; 1470 DeHaro Street, San Francisco, CA 94107 (US).

(74) Agents: LANG, Dan, H. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111–3834 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE ELECTRONIC COMMERCE EMPLOYING INTEGRATED CIRCUIT CARDS



(57) Abstract

A system for network–based electronic commerce employing integrated circuit cards (234) is provided. In one embodiment, cardholder authentication is provided by use of on–card symmetric cryptographic processing. The cardholder thus need not be limited to performing transactions from any particular computer system. Asymmetric cryptographic techniques are employed for communication of transaction data over the network (110).

*(Referred to in PCT Gazette No. 08/1999, Section II)

BNSDOCID: <WO___9840982A1_IA>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURE ELECTRONIC COMMERCE EMPLOYING INTEGRATED CIRCUIT CARDS

STATEMENT OF RELATED APPLICATIONS

This application claims priority from U.S. Provisional Application No. 60/040,958 filed on March 12, 1997, the contents of which are herein incorporated by reference.

BACKGROUND OF THE INVENTION

The present invention relates to electronic commerce and more particularly to systems and methods for using a network for electronic commerce.

The Internet is a new means by which consumers can access and purchase information, communicate and pay for services, and acquire and pay for goods. Because of the anonymous nature of communication networks, new methods and systems must be developed to substitute for existing procedures used in face-to-face or mail order/telephone order transactions. These methods and systems should provide confidential transmission, authentication of parties involved, and assurance of the integrity of payment instructions for goods and services.

To achieve these objectives and others, the Secure Electronic Transaction (SET) Specification has been developed. The SET protocol allows customers to make payment card transactions securely over the Internet. However, transactions made using this protocol generally involve an initial cardholder registration process that requires account data to be entered manually (e.g., via a keyboard at the cardholder's personal computer (PC)). The SET protocol supports several levels of security, some of which are only accessible if cardholder-related data is stored on the cardholder access device, generally limiting the availability of such security to the cardholder's own PC. The use of SET does not allow the issuer to authenticate that a card was present or that the cardholder was genuine when authorizing payment transactions.

What is needed is a system that enhances transaction security over the Internet by verifying presence of a card while providing freedom to the user to initiate transactions from multiple card access devices.

SUMMARY OF THE INVENTION

By virtue of the present invention, a system for network-based electronic commerce employing integrated circuit cards is provided. In one embodiment, cardholder authentication is provided by use of on-card symmetric cryptographic processing. The cardholder thus need not be limited to performing transactions from any particular computer system. Asymmetric cryptographic techniques are employed for communication of transaction data over the network.

According to a first embodiment of the present invention, a computer-implemented method for processing transactions over a network is provided. The method includes steps of: establishing a connection between a card access device coupled to the network and an integrated circuit card, transferring a cryptogram generation command comprising challenge data from the card access device to the integrated circuit card, in response to the cryptogram generation command, using the integrated circuit card to encrypt the challenge data to form a response, transferring the response from the integrated circuit card to the card access device, forming a payment instruction message at the card access device, the payment instruction message including the response, encrypting at least a portion of the payment instruction message using asymmetric cryptographic techniques.

A second embodiment of the present invention provides a computer program product for facilitating secure electronic commerce. The product is for use with a computer coupled to a network and a card reading device. The product includes: code for establishing a connection between the computer and an integrated circuit card in communication with the card reading device, code for transferring a cryptogram generation command comprising challenge data from the computer to the integrated circuit card, code for receiving a response to the cryptogram generation command from the integrated circuit card, code for forming a payment instruction message, the payment instruction message including the response, and a computer-readable medium for storing the codes.

A third embodiment of the present invention provides an integrated circuit card. The integrated circuit card includes: an interface for receiving external commands and data, a symmetric cryptographic processor that encrypts a challenge value received via the interface to form a response to transmit via the interface, an asymmetric cryptographic processor that encrypts a value received from the interface using a private

key unique to the integrated circuit card, and a memory storing the key and a certificate including a public key matching the private key unique to the integrated circuit card, the public key being signed by a private key of a certificate authority.

A further understanding of the nature and advantages of the inventions herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts a general architecture for electronic commerce according to one embodiment of the present invention.

Fig. 2 depicts a computer system suitable for use with the present invention.

Fig. 3 depicts an integrated circuit card according to one embodiment of the present invention.

Fig. 4 is a top-level flowchart describing steps of transaction processing according to one embodiment of the present invention.

DESCRIPTION OF SPECIFIC EMBODIMENTS

The discussion that follows assumes a familiarity with cryptographic techniques. A good general reference is Schneier, Applied Cryptography Second Edition (John Wiley & Sons, 1996), the contents of which are herein incorporated by reference.

Fig. 1 depicts a general architecture for electronic commerce according to one embodiment of the present invention. A cardholder employs a cardholder access device (CAD) 102 to order merchandise, services, or information from a merchant that operates a merchant server system 104. CAD 102 includes a card reading device 106. CAD 102 may be, for example, a cardholder's PC or a public kiosk.

Payment for the cardholder's order is arranged through a payment gateway 108. Payment gateway 108 in turn interacts with other computer systems such as an acquirer server 109. These other computer systems are not shown. Communication among merchant server 104, payment gateway 108, and CAD 102 is preferably through the Internet 110. A private connection is used between payment gateway 108 and acquirer server 109.

Merchant server 104 is a system that interfaces with CAD 102 to offer goods or services in return for electronic payment. Merchant server 104 interfaces with payment gateway 108 to process electronic commerce transactions. Payment gateway 108 is a logical entity that provides electronic commerce services to the merchants in support an acquirer and interfaces to acquirer server 109 to support the authorization and capture of electronic commerce transactions. The acquirer is typically a financial institution that supports merchants by providing services for processing electronic transactions.

Acquirer server 109 in turn interacts with a card issuer 112. According to one embodiment of the present invention, card issuer 112 helps authenticate a card inserted into integrated circuit card 106. Issuer 112 and payment gateway 108 preferably interact through a private network 114 rather than the Internet 110.

In a preferred embodiment, interaction among CAD 102, merchant server 104, and payment gateway 108 is defined in part according to the SET Secure Electronic Transaction Specification (Version 1.0 May 31, 1997) published by Visa, the assignee of the present application, and MasterCard. This document will be referred to herein as the "SET Specification" and incorporated by reference for all purposes.

Fig. 2 depicts a computer system suitable for use with the present invention. Fig. 2 shows basic subsystems of a computer system 200 suitable for use with the present invention. Computer system 200 may represent the implementation of payment gateway 108, merchant server 104, or CAD 102. In Fig. 2, computer system 200 includes a bus 212 which interconnects major subsystems such as a central processor 214, a system memory 216, an input/output controller 218, a CD-ROM player 220 operative to receive a CD-ROM 222, a display screen 224 via a display adapter 226, a serial port 228, a keyboard 230, a storage interface 231 connected to a fixed disk drive 232, and a floppy disk drive 233 operative to receive a floppy disk 233A. Many other devices may be connected such as a mouse 236 connected to serial port 228 or a network interface 238 through another serial port 240. Many other devices or subsystems (not shown) may be connected in a similar manner. Also, it is not necessary for all of the devices shown in Fig. 2 to be present to practice the present invention, as discussed below. The devices and subsystems may be interconnected in different ways from that shown in Fig. 2. The operation of a computer system such as that shown in Fig. 2 is readily known in the art and is not discussed in detail in the present application.

Source code to implement the present invention may be operably disposed in system memory 216 or stored on storage media such as fixed disk 232 or floppy disk 233A, fixed disk 232, or CD-ROM 232.

When computer system 200 implements a CAD, card reading device 106 is also connected as part of computer system 200. Card reading device 106 may accept an integrated circuit card (ICC) 234.

Fig. 3 depicts ICC 234 according to one embodiment of the present invention. Various mechanical and electrical characteristics of ICC 234 and aspects of its interaction with card reading device 106 are defined by the following specifications, all of which are herein incorporated by reference.

Visa Integrated Circuit Card Specification, (Visa International Service Association 1996).

EMV Integrated Circuit Card Specification for Payment Systems, (Visa International Service Association 1996).

EMV Integrated Circuit Card Terminal Specification for Payment Systems, (Visa International Service Association 1996).

EMV Integrated Circuit Card Application Specification for Payment Systems, (Visa International Service Association 1996).

International Standard: Identification Cards -- Integrated Circuit(s) Cards with Contacts, Parts 1-6 (International Standards Organization 1987-1995).

Besides the electronic commerce features discussed in the present application, ICC 234 may provide the functionality of a credit card, debit card, ATM card, stored value card, identification card, etc. ICC 234 includes electrical contacts 302 for receiving power and exchanging information with card reading device 106. A magnetic stripe 304 allows storage of information for reading by magnetic stripe readers. An integrated circuit 306 includes a processor and memory for storing application information. An embossing area 308 is available for imprinting the cardholder name, account number, and expiration date.

The combination of memory and processor preferably implements a symmetric cryptographic processor and in certain embodiments an asymmetric cryptographic processor. The symmetric cryptographic processor preferably uses the DES algorithm to encrypt an externally generated value employing a symmetric key. The asymmetric cryptographic processor preferably uses the RSA algorithm to encrypt an

externally generated value employing a private asymmetric key. The symmetric key and asymmetric key are preferably stored in memory so as to be inaccessible to external devices interacting with integrated circuit card 234.

The use of SET ensures the integrity and authenticity of cardholder account data transmitted through the Internet and does not require the use of an ICC or any physical payment card to initiate a purchase transaction. SET defines the transmission of a digital signature from CAD 102 to merchant server 104 and payment gateway 108 to ensure that the data transmitted from the cardholder has not been changed. According to the present invention, this digital signature operation may be performed either by CAD 102 or by ICC 234. In conjunction with the digital signatures, the SET protocol allows the transmission of a certificate chain to the merchant, validating a relationship between the cardholder and issuer. According to the present invention, this certificate chain, if used, may be stored either on CAD 102 or on ICC 234.

According to SET, cardholder certificates function as electronic representation of a payment card. Each cardholder certificate is digitally signed by a financial institution using the private key of the financial institution. Thus the cardholder certificate can only be generated by a financial institution and cannot be altered by a third party. The cardholder certificate includes the public signature key of the cardholder, and a hash of the cardholder's account information and secret value known to the SET software operating on CAD 102. All of this data is signed with the private signature key of the financial institution. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. SET does not mandate the use of cardholder certificates but allows for their use to enhance security.

The cardholder certificate is verifiable through a hierarchy of trust. The cardholder certificate is linked to a signature certificate of the entity, a cardholder certificate authority (CCA), that digitally signed the cardholder certificate. The signature certificate of the CCA includes the public signature key of the CCA signed by geopolitical certificate authority (GCA) with its own private signature key. The CCA certificate is linked to a GCA certificate which includes the public signature key of the GCA signed by the payment brand (e.g., Visa, MasterCard, etc.) with its private signature key. The GCA certificate is linked to a payment brand certificate that includes the public signature key of the payment brand as signed by a root authority with its

private signature key. The payment brand certificate is in turn linked to a root authority certificate which includes the root's public signature key signed by the root's private key.

For each payment brand, there may be a GCA for each country. A recipient of the cardholder certificate will be able to verify it using the public signature key of the CCA. The public signature key of the CCA is verifiable by use of the public signature key of the GCA to decrypt the CCA certificate. In turn, the public signature key of the GCA is verifiable by using the payment brand public key to decrypt the GCA certificate. The payment brand public signature key is verifiable by using the root public signature key to decrypt the payment brand certificate. Thus, a merchant may verify a cardholder by traversing the certificate chain. SET provides for the certificate chain to be maintained on CAD 102. According to the present invention, the certificate chain may also be stored on ICC 234.

In one embodiment, the present invention augments the protections provided by SET using on-line authorization by issuer 112. Integrated circuit card 234 generates an authorization request cryptogram (ARQC) which is used by issuer 112 to authenticate the card.

The discussion that follows refers to three exemplary embodiments. In a first embodiment referred to as "Option 1," integrated circuit card 234 incorporates asymmetric cryptographic processing and stores a cardholder certificate and the chain of certificates leading from the cardholder certificate to the root. In a second embodiment referred to as "Option 2," integrated circuit card 234 does not incorporate asymmetric cryptographic processing and does not store the cardholder certificate and the other certificates of the chain. In "Option 2," however, a cardholder certificate and certificate chain are associated with integrated circuit but stored on CAD 102 which is capable of asymmetric cryptographic processing. In a third embodiment referred to as "Option 3," integrated circuit card 234 does not incorporate asymmetric cryptographic processing and does not store the cardholder certificate and the other certificates of the chain. Also, there is no cardholder certificate associated with this card and stored by CAD 102.

Fig. 4 is a top-level flowchart describing steps of transaction processing according to one embodiment of the present invention. Prior to processing of the transaction, at step 402, the cardholder shops, e.g., by browsing through the merchant's website. CAD 102 may be equipped with an HTTP-compatible browser to facilitate viewing catalog information stored on merchant server 104. At step 404, after the user

has decided to purchase particular goods or services, he or she initiates a request, e.g., by selecting a link or screen button within the browser. Merchant server 104 receives the request and responds by sending CAD 102 a merchant certificate and a payment gateway certificate at step 406. The merchant certificate includes the public key-exchange key of the merchant. The payment gateway certificate includes the public key-exchange key of the payment gateway. These certificates are signed with the private keys of CCAs to which the merchant and payment gateway are assigned. At step 408, software on CAD 102 verifies the merchant and payment gateway certificates by traversing the certificate chain to the root key.

At step 410, CAD 102 checks for the presence of integrated circuit card 234 in card reading device 106. If integrated circuit card 234 is not present, further operation is in accordance with SET techniques at step 412. If integrated circuit card 234 is present, processing proceeds to step 414 where CAD 102 selects the particular application on integrated circuit card 234 that incorporates the features of the present invention. According to the various EMV Specifications and the VIS Specification, integrated circuit card 234 may support multiple applications. If integrated circuit card 234 operates according to the VIS specification, the selected application is preferably a credit/debit application and there need not be a separate application defined for networked electronic commerce.

At step 416, initial application processing functions are performed between CAD 102 and integrated circuit card 234. CAD 102 issues a command to integrated circuit card 234 to retrieve a list of files and records stored on the card and related to the selected application. This command also retrieves a list of functions supported by the selected application. This list will indicate whether integrated circuit card 234 supports cardholder verification.

At step 417, CAD 102 sends a purchase initialization request to merchant server 104 in accordance with SET. The purchase initialization request includes the brand of integrated circuit card 234, e.g., "Visa." In response, merchant server 104 sends a purchase initialization request response to CAD 102. The purchase initialization request response preferably includes a transaction identifier uniquely identifying the transaction among other data specified by SET.

At step 418, CAD 102 retrieves the listed files and records associated with the selected application from integrated circuit card 234. The retrieved information

includes the cardholder's personal account number (PAN) and expiration date. For Option 1 cards, CAD 102 reads the cardholder certificate and certificate chain from integrated circuit card 234. According to the present invention, integrated circuit card 234 may also store a URL identifying a network address of the payment brand. CAD 102 retrieves this URL and accesses the identified network address to retrieve and display images identifying the card issuer and payment brand.

At step 420, CAD 102 performs cardholder verification if this is supported by integrated circuit card 234. Included in the files and records retrieved at step 418 is a list of cardholder verification methods supported by the card. The preferred method of cardholder verification is offline PIN processing. If CAD 102 also supports offline PIN processing, the cardholder is prompted for entry of his or her PIN. CAD 102 sends the entered PIN as cleartext to integrated circuit card 234. Integrated circuit card 234 compares the entered PIN with a reference PIN and returns the results of the comparison to CAD 102. CAD 102 records whether offline PIN processing was performed, whether a PIN was actually entered, and the results of the comparison to the reference PIN.

Step 422 begins an on-line authorization procedure where issuer 112 may verify the authenticity of integrated circuit card 234. CAD 102 requests generation of an authorization request cryptogram (ARQC) if PIN entry was successful, or an application authorization cryptogram (AAC) if PIN entry was not successful. A request for an AAC is tantamount to declining the transaction. The request for an ARQC or AAC includes variable data particular to the transaction, preferably including an amount authorized by the merchant, a transaction currency code previously supplied by the merchant, transaction date, and an unpredictable number.

In response to the request for an ARQC, integrated circuit card 234 preferably performs various card risk management functions including checking for previous authentication failures, PIN entry results, and other risk factors. If an AAC has been requested by CAD 102 or any of the risk factors are present, integrated circuit card 234 returns an AAC to CAD 102. CAD 102 responds to the AAC by terminating the transaction. If an ARQC has been requested and integrated circuit card 234 previously successfully performed the PIN comparison, integrated circuit card 234 responds by returning an ARQC.

Both an ARQC and an AAC preferably include the variable data listed above encrypted with a symmetric key unique to integrated circuit card 234. In a

preferred embodiment, the encryption algorithm is DES. Ultimately, the ARQC is sent to issuer 112 for on-line authentication of the card. Receipt of an AAC by CAD 102 result in termination of the transaction.

The unpredictable number is formed by CAD 102 through the following process. The transaction identifier, which is preferably a 20 byte value is divided into five 4-byte blocks. The first (leftmost) block is exclusive-ORed with the second block. The result of this first exclusive OR operation is exclusive-ORed with the third block. The result of the second exclusive OR operation is exclusive-ORed with the fourth block. The result of the third exclusive OR operation is exclusive-ORed with the fifth (rightmost) block to form the unpredictable number.

How CAD 102 formulates a purchase request to the merchant will depend on whether this is an Option 1, Option 2, or Option 3 system. At step 424, CAD 102 checks whether SET-related data including the cardholder certificate chain and a value known as the PAN secret are stored on integrated circuit card 234 indicating that the card is configured for Option 1. The PAN secret is the result of exclusive-ORing an arbitrary number associated with the card with an arbitrary number associated with the issuer. If the card is configured for Option 1, formulation of the purchase request occurs at step 426.

If the card is not configured for Option 1, CAD 102 checks at step 428 to see if it has the cardholder certificate chain and PAN secret internally stored, indicating an Option 2 system. If this is an Option 2 system, the purchase request is formulated at step 430. If the cardholder certificate chain and PAN secret are present on neither integrated circuit card 234 nor CAD 102, this indicates an Option 3 system and the purchase request is formulated at step 432.

According to SET, a purchase request includes two parts, order information (OI) and payment instructions (PI). The OI identifies the order to the merchant. The PI is not reviewed by the merchant but is instead forwarded to payment gateway 108. When a cardholder certificate is available, SET provides for generation of a dual signature for the OI and PI. Message digests for both the OI and PI are generated and concatenated. The message digest of the concatenation result is generated and encrypted using the cardholder private signature key to form a dual signature. The PI is encrypted with a randomly generated symmetric key. This randomly generated symmetric key along with the cardholder's account information is encrypted with the

private key-exchange key of the payment gateway. The purchase request as sent to the merchant includes the encrypted PI and OI. The purchase request also includes the cardholder certificate chain.

In the case of Option 1 processing at step 426, CAD 102 creates the PI and OI as defined by the SET Specification. Where the personal account number and expiration date would normally appear in the PI, CAD 102 includes a series of zeroes. CAD 102 forms a special data object including certain integrated circuit card-related data. This data includes the ARQC and the cleartext data encrypted within the ARQC including the unpredictable number. This special data object is embedded in the PI. All of the steps of generating the purchase request are performed by CAD 102 except for encrypting the message digest of the concatenation result using the cardholder private key. This step is performed by integrated circuit card 234. In a preferred embodiment where integrated circuit card 234 conforms to the VIS specification, this encryption is performed using the INTERNAL AUTHENTICATE command included in the specification.

Option 2 processing at step 430 is the same as Option 1 processing at step 426, except that all steps of forming the purchase request are now performed by CAD 102 including encrypting the message digest of the concatenation result using the cardholder private key.

In the case of Option 3 processing at step 432, CAD 102 creates the PI and OI as defined by the SET specification. As with Option 1 and Option 3, the integrated circuit card-related data is included with the PI. However, no dual signature is created for the payment request.

At step 434, CAD 102 sends the purchase request to merchant server 104. At this time, integrated circuit card 234 is no longer needed to complete the transaction and CAD 102 may prompt the cardholder to remove his or her card from card reading device 106.

At step 436, merchant server 104 processes the purchase request in accordance with SET. A portion of the purchase request is the PI which is forwarded to payment gateway 108.

At step 438, payment gateway 108 processes the PI. Payment gateway 108 decrypts the PI using its private key-exchange key. After decrypting the PI, payment gateway 108 checks for the card-related data in the PI to determine if the

purchase request involved use of an integrated circuit card. Once this has been verified, payment gateway 108 recalculates the unpredictable number from the transaction identifier and the merchant identifier it obtains from the ARQC. The result is compared with the unpredictable number transmitted within the PI. If there is no match, the transaction is rejected. The PAN and card expiration date are decrypted.

Payment gateway 108 sends issuer 112 via acquirer server 109 an authorization request that includes the data related to the payment transaction. The authorization request also preferably includes information indicating whether or not SET certificates were used and whether these certificates were present on integrated circuit card 234. Issuer 112 is aware of the unique symmetric key of the cardholder and attempts to verify the ARQC from the cleartext information included in the integrated circuit card related data. Issuer 112 applies the unique cardholder key to symmetrically encrypt the cleartext information and obtain ARQC'. If ARQC' matches ARQC, issuer 112 sends an authorization response message to payment gateway 108 indicating that the transaction is authorized by issuer 112. Payment gateway 108 responds to receipt of this authorization request message by sending an authorization message to merchant server 104. Merchant server 104 may then fulfill the order.

The card authentication operation of user 118 provides security that enhances or substitutes for the protection offered by the SET cardholder certificate. This security is potentially available to the cardholder through multiple acceptance devices, offering portability unavailable with prior art networked electronic commerce technologies.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereunto without departing from the broader spirit and scope of the invention as set forth in the appended claims and their full scope of equivalents. For example, the specification has discussed enhancements to the EMV, VIS, and SET specifications. The present invention is not, however, limited to use with any particular protocol or specification for cards electronic commerce.

WHAT IS CLAIMED IS:

1. A computer-implemented method for processing transactions over a network comprising the steps of:

establishing a connection between a card access device coupled to said network and an integrated circuit card;

transferring a cryptogram generation command comprising challenge data from said card access device to said integrated circuit card;

in response to said cryptogram generation command, using said integrated circuit card to encrypt said challenge data to form a response;

transferring said response from said integrated circuit card to said card access device;

forming a payment instruction message at said card access device, said payment instruction message comprising said response; and

encrypting at least a portion of said payment instruction message using asymmetric cryptographic techniques.

2. The method of claim 1 further comprising the step of sending said encrypted payment instruction message from said card access device to a merchant via said network.

3. The method of claim 1 wherein said step of encrypting said payment instruction message comprises using a symmetric key to encrypt said at least a portion of said payment instruction message and encrypting said symmetric key with a public key of a payment processor.

4. The method of claim 1 further comprising the steps of:

forming an order information message at said card access device;

hashing said order information message to obtain a digest of said order information message;

hashing said payment instruction message to obtain a digest of said payment instruction message;

concatenating said digest of said order information message and said digest of said payment instruction message to obtain a concatenated digest; and

encrypting said concatenated digest with a private signature key particular to said integrated circuit card to obtain a signed concatenated digest.

5. The method of claim 4 wherein said encrypting said concatenated digest step is performed by said integrated circuit card.

6. The method of claim 4 wherein said encrypting said concatenated digest step is performed by said card access device.

7. The method of claim 1 wherein said challenge comprises an unpredictable number.

8. The method of claim 1 wherein said unpredictable number is derived from an identifier identifying a particular merchant and an identifier identifying a particular transaction.

9. A computer program product for use with a computer coupled to a network and a card reading device facilitating secure electronic commerce, said computer program product comprising:

code for establishing a connection between said computer and an integrated circuit card in communication with said card reading device;

code for transferring a cryptogram generation command comprising challenge data from said computer to said integrated circuit card;

code for receiving a response to said cryptogram generation command from said integrated circuit card;

code for forming a payment instruction message, said purchase instruction message comprising said response; and

a computer-readable medium for storing the codes.

10. The computer program product of claim 9 further comprising code for encrypting said payment instruction message using asymmetric cryptographic techniques.

11. The computer program product of claim 10 further comprising the step of sending said encrypted payment instruction message from said card access device to a merchant via said network.

12. The computer program product of claim 10 wherein said code for encrypting said payment instruction message comprises code for using a symmetric key to encrypt said payment instruction message and encrypting said symmetric key with a public key of a payment processor.

13. The computer program product of claim 9 further comprising:

code for forming an order information message at said card access device;

code for hashing said order information message to obtain a digest of said order information message;

code for hashing said payment instruction message to obtain a digest of said payment instruction message;

code for concatenating said digest of said order information message and said digest of said payment instruction message to obtain a concatenated digest; and

code for encrypting said concatenated digest with a secret signature key particular to said integrated circuit card to obtain a signed concatenated digest.

14. An integrated circuit card comprising:

an interface for receiving external commands and data;

a symmetric cryptographic processor that encrypts a challenge value received via said interface to form a response to transmit via said interface;

an asymmetric cryptographic processor that encrypts a value received from said interface using a private key unique to said integrated circuit card; and

a memory storing said key and a certificate comprising a public key matching said private key unique to said integrated circuit card, said public key being signed by a private key of a certificate authority.

15. The integrated circuit card of claim 14 wherein said key is inaccessible to said interface.

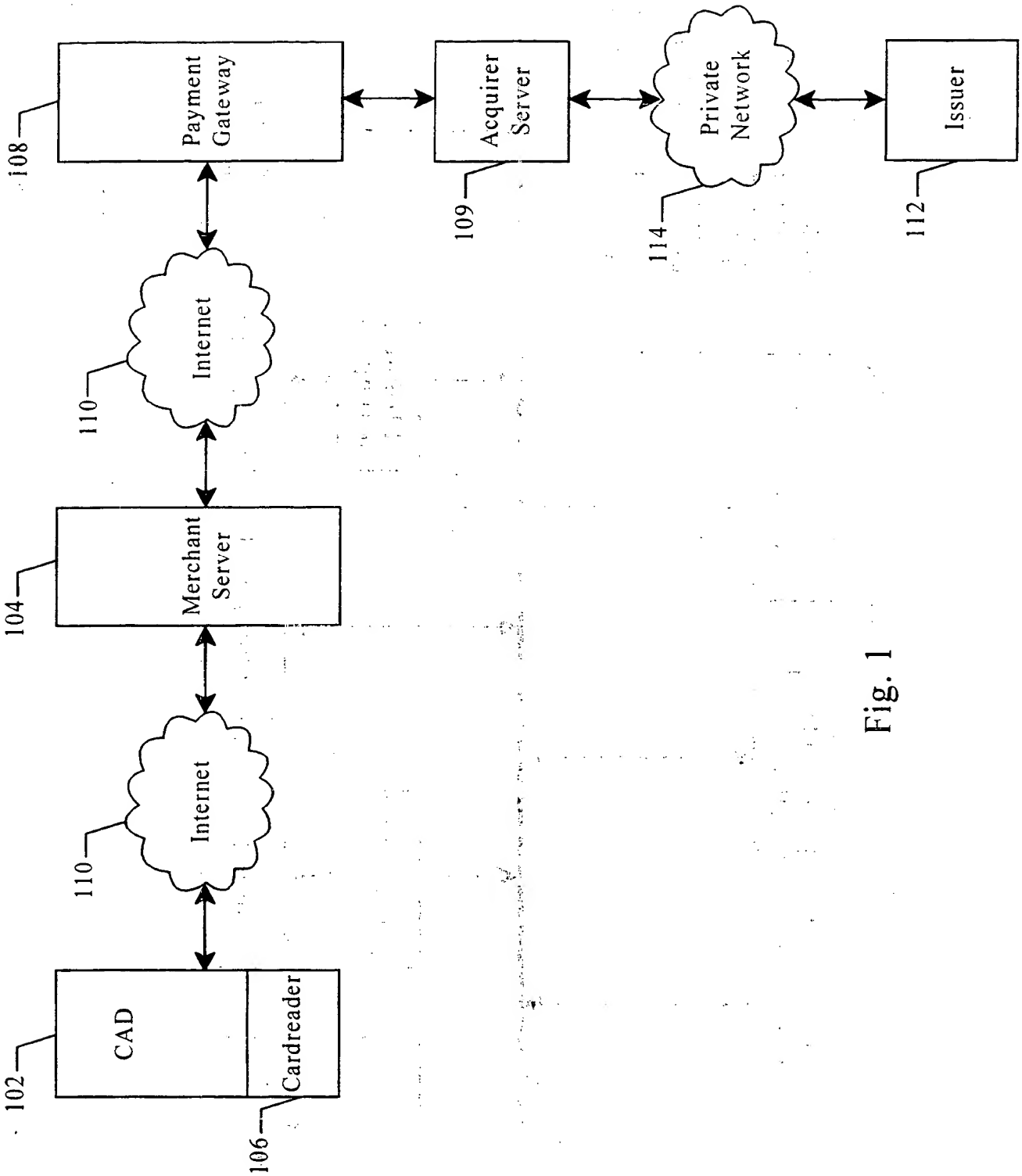


Fig. 1

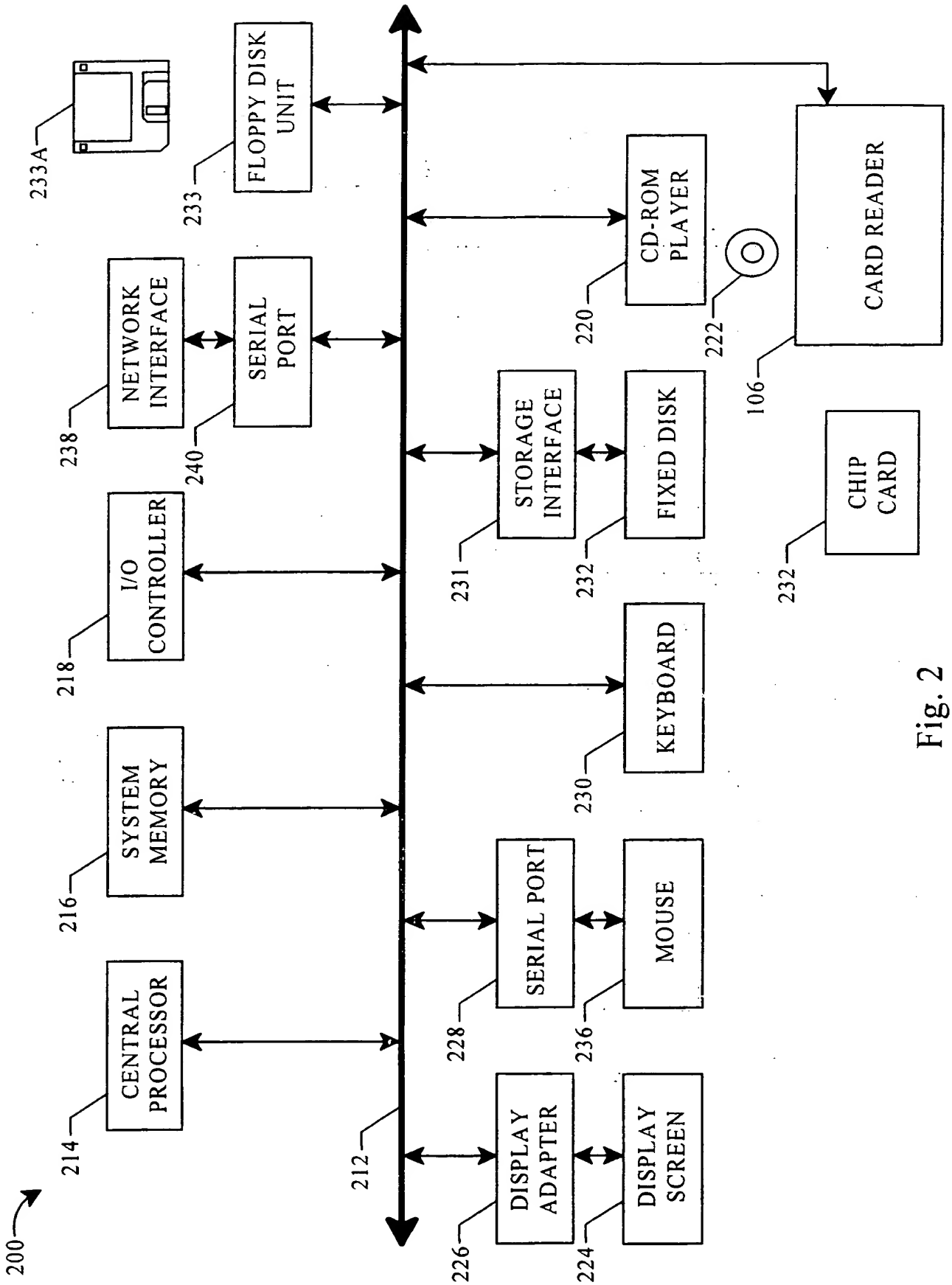


Fig. 2

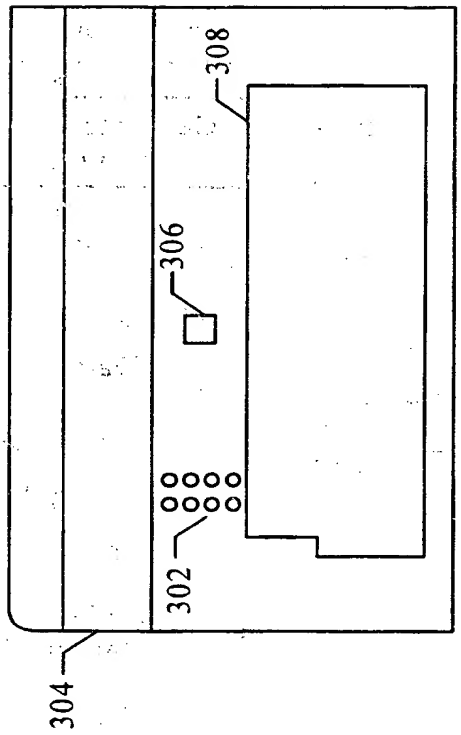


Fig. 3

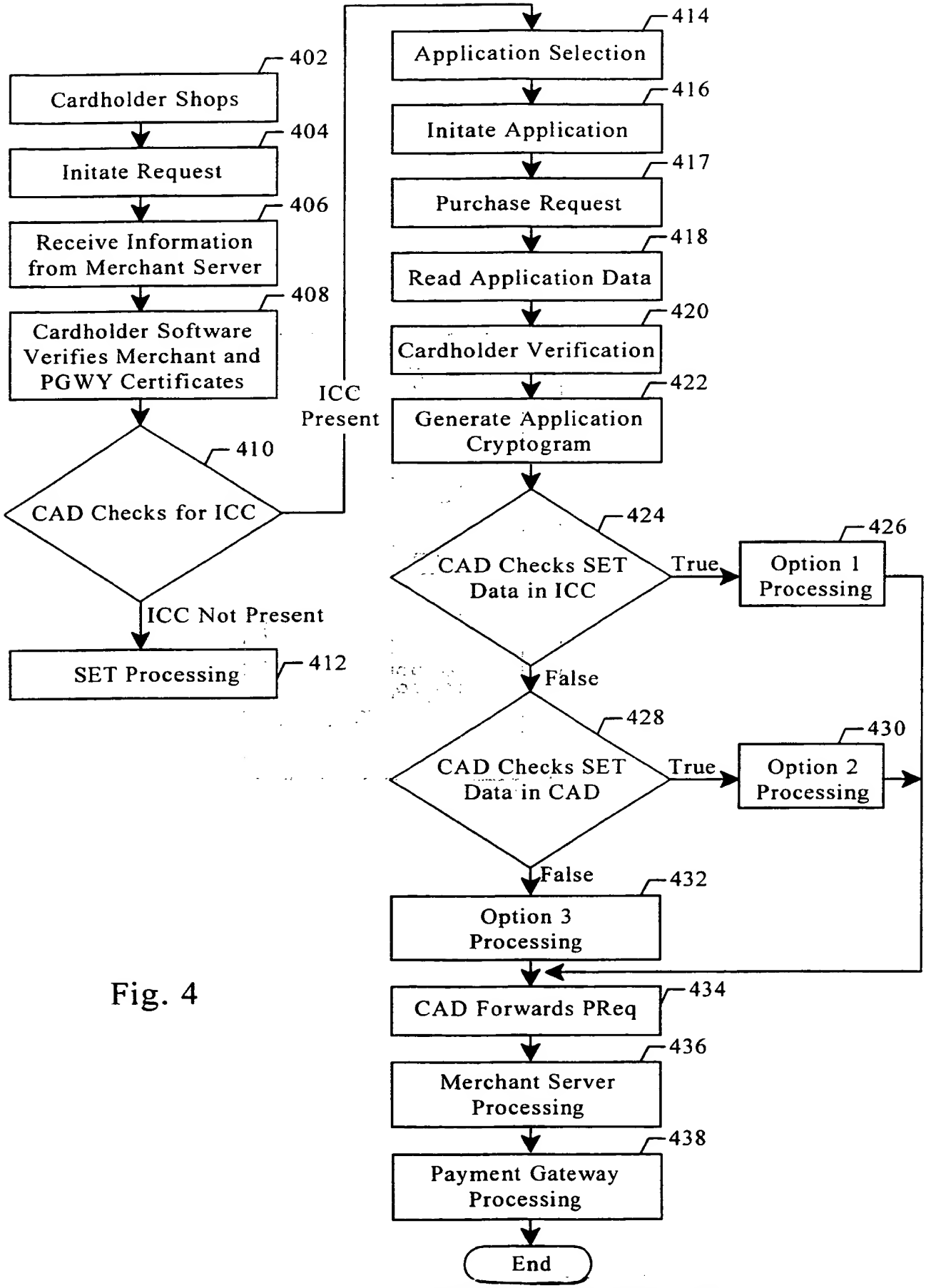


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/04606

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04K 1/00; H04L 9/00
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 49, 23, 24, 21, 28, 29, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 5,754,656 A (NISHIOKA, et al.) 19 May 1998 (19/05/98).	1-15
A, P	US 5,742,756 A (DILLAWAY, et al.) 21 April, 1998 (21/04/98).	1-15
A, P	US 5,721,781 A (DEO, et al.) 24 February 1998 (24/02/98).	1-15
A, P	US 5,706,349 (ADITHAM, et al.)06 January 1998 (06/01/98).	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 JUNE 1998	Date of mailing of the international search report 08 JUL 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/04606

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

380/25, 49

THIS PAGE BLANK (USPTO)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00, H04L 9/00

A1

(11) International Publication Number: **WO 98/40982**

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/US98/04606

(22) International Filing Date: 10 March 1998 (10.03.98)

(30) Priority Data:
60/040,958 12 March 1997 (12.03.97) US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US 60/040,958 (CIP)
Filed on 12 March 1997 (12.03.97)

(71) Applicant *(for all designated States except US)*: VISA INTERNATIONAL [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US).

(72) Inventors; and

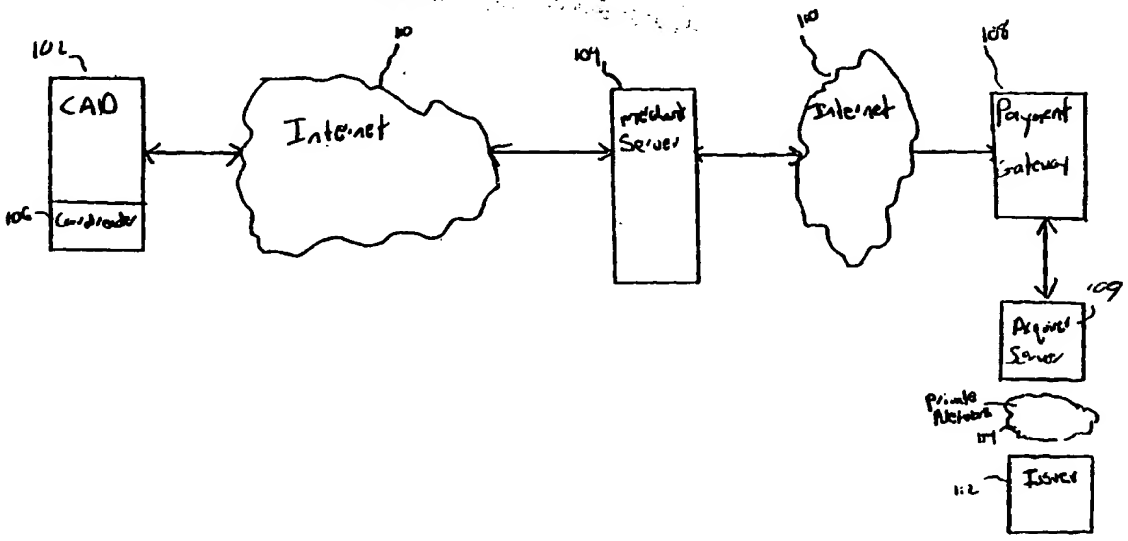
(75) Inventors/Applicants *(for US only)*: KEATHLEY, Kimberly, Ann [US/US]; 18552 Center Street, Castro Valley, CA 94546 (US). CHEN, Ann–Pin [US/US]; 600 Somerset Lane, Foster City, CA 94404 (US). MCCUSKER, Nancy [US/US]; 1470 DeHaro Street, San Francisco, CA 94107 (US).

(74) Agents: LANG, Dan, H. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111–3834 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE ELECTRONIC COMMERCE EMPLOYING INTEGRATED CIRCUIT CARDS



(57) Abstract

A system for network–based electronic commerce employing integrated circuit cards (234) is provided. In one embodiment, cardholder authentication is provided by use of on–card symmetric cryptographic processing. The cardholder thus need not be limited to performing transactions from any particular computer system. Asymmetric cryptographic techniques are employed for communication of transaction data over the network (110).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURE ELECTRONIC COMMERCE EMPLOYING INTEGRATED CIRCUIT CARDS

STATEMENT OF RELATED APPLICATIONS

This application claims priority from U.S. Provisional Application No. 60/040,958 filed on March 12, 1997, the contents of which are herein incorporated by reference.

BACKGROUND OF THE INVENTION

The present invention relates to electronic commerce and more particularly to systems and methods for using a network for electronic commerce.

The Internet is a new means by which consumers can access and purchase information, communicate and pay for services, and acquire and pay for goods. Because of the anonymous nature of communication networks, new methods and systems must be developed to substitute for existing procedures used in face-to-face or mail order/telephone order transactions. These methods and systems should provide confidential transmission, authentication of parties involved, and assurance of the integrity of payment instructions for goods and services.

To achieve these objectives and others, the Secure Electronic Transaction (SET) Specification has been developed. The SET protocol allows customers to make payment card transactions securely over the Internet. However, transactions made using this protocol generally involve an initial cardholder registration process that requires account data to be entered manually (e.g., via a keyboard at the cardholder's personal computer (PC)). The SET protocol supports several levels of security, some of which are only accessible if cardholder-related data is stored on the cardholder access device, generally limiting the availability of such security to the cardholder's own PC. The use of SET does not allow the issuer to authenticate that a card was present or that the cardholder was genuine when authorizing payment transactions.

What is needed is a system that enhances transaction security over the Internet by verifying presence of a card while providing freedom to the user to initiate transactions from multiple card access devices.

SUMMARY OF THE INVENTION

By virtue of the present invention, a system for network-based electronic commerce employing integrated circuit cards is provided. In one embodiment, cardholder authentication is provided by use of on-card symmetric cryptographic processing. The cardholder thus need not be limited to performing transactions from any particular computer system. Asymmetric cryptographic techniques are employed for communication of transaction data over the network.

According to a first embodiment of the present invention, a computer-implemented method for processing transactions over a network is provided. The method includes steps of: establishing a connection between a card access device coupled to the network and an integrated circuit card, transferring a cryptogram generation command comprising challenge data from the card access device to the integrated circuit card, in response to the cryptogram generation command, using the integrated circuit card to encrypt the challenge data to form a response, transferring the response from the integrated circuit card to the card access device, forming a payment instruction message at the card access device, the payment instruction message including the response, encrypting at least a portion of the payment instruction message using asymmetric cryptographic techniques.

A second embodiment of the present invention provides a computer program product for facilitating secure electronic commerce. The product is for use with a computer coupled to a network and a card reading device. The product includes: code for establishing a connection between the computer and an integrated circuit card in communication with the card reading device, code for transferring a cryptogram generation command comprising challenge data from the computer to the integrated circuit card, code for receiving a response to the cryptogram generation command from the integrated circuit card, code for forming a payment instruction message, the payment instruction message including the response, and a computer-readable medium for storing the codes.

A third embodiment of the present invention provides an integrated circuit card. The integrated circuit card includes: an interface for receiving external commands and data, a symmetric cryptographic processor that encrypts a challenge value received via the interface to form a response to transmit via the interface, an asymmetric cryptographic processor that encrypts a value received from the interface using a private

key unique to the integrated circuit card, and a memory storing the key and a certificate including a public key matching the private key unique to the integrated circuit card, the public key being signed by a private key of a certificate authority.

A further understanding of the nature and advantages of the inventions herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts a general architecture for electronic commerce according to one embodiment of the present invention.

Fig. 2 depicts a computer system suitable for use with the present invention.

Fig. 3 depicts an integrated circuit card according to one embodiment of the present invention.

Fig. 4 is a top-level flowchart describing steps of transaction processing according to one embodiment of the present invention.

DESCRIPTION OF SPECIFIC EMBODIMENTS

The discussion that follows assumes a familiarity with cryptographic techniques. A good general reference is Schneier, Applied Cryptography Second Edition (John Wiley & Sons, 1996), the contents of which are herein incorporated by reference.

Fig. 1 depicts a general architecture for electronic commerce according to one embodiment of the present invention. A cardholder employs a cardholder access device (CAD) 102 to order merchandise, services, or information from a merchant that operates a merchant server system 104. CAD 102 includes a card reading device 106. CAD 102 may be, for example, a cardholder's PC or a public kiosk.

Payment for the cardholder's order is arranged through a payment gateway 108. Payment gateway 108 in turn interacts with other computer systems such as an acquirer server 109. These other computer systems are not shown. Communication among merchant server 104, payment gateway 108, and CAD 102 is preferably through the Internet 110. A private connection is used between payment gateway 108 and acquirer server 109.

Merchant server 104 is a system that interfaces with CAD 102 to offer goods or services in return for electronic payment. Merchant server 104 interfaces with payment gateway 108 to process electronic commerce transactions. Payment gateway 108 is a logical entity that provides electronic commerce services to the merchants in support an acquirer and interfaces to acquirer server 109 to support the authorization and capture of electronic commerce transactions. The acquirer is typically a financial institution that supports merchants by providing services for processing electronic transactions.

Acquirer server 109 in turn interacts with a card issuer 112. According to one embodiment of the present invention, card issuer 112 helps authenticate a card inserted into integrated circuit card 106. Issuer 112 and payment gateway 108 preferably interact through a private network 114 rather than the Internet 110.

In a preferred embodiment, interaction among CAD 102, merchant server 104, and payment gateway 108 is defined in part according to the SET Secure Electronic Transaction Specification (Version 1.0 May 31, 1997) published by Visa, the assignee of the present application, and MasterCard. This document will be referred to herein as the "SET Specification" and incorporated by reference for all purposes.

Fig. 2 depicts a computer system suitable for use with the present invention. Fig. 2 shows basic subsystems of a computer system 200 suitable for use with the present invention. Computer system 200 may represent the implementation of payment gateway 108, merchant server 104, or CAD 102. In Fig. 2, computer system 200 includes a bus 212 which interconnects major subsystems such as a central processor 214, a system memory 216, an input/output controller 218, a CD-ROM player 220 operative to receive a CD-ROM 222, a display screen 224 via a display adapter 226, a serial port 228, a keyboard 230, a storage interface 231 connected to a fixed disk drive 232, and a floppy disk drive 233 operative to receive a floppy disk 233A. Many other devices may be connected such as a mouse 236 connected to serial port 228 or a network interface 238 through another serial port 240. Many other devices or subsystems (not shown) may be connected in a similar manner. Also, it is not necessary for all of the devices shown in Fig. 2 to be present to practice the present invention, as discussed below. The devices and subsystems may be interconnected in different ways from that shown in Fig. 2. The operation of a computer system such as that shown in Fig. 2 is readily known in the art and is not discussed in detail in the present application.

Source code to implement the present invention may be operably disposed in system memory 216 or stored on storage media such as fixed disk 232 or floppy disk 233A, fixed disk 232, or CD-ROM 232.

When computer system 200 implements a CAD, card reading device 106 is also connected as part of computer system 200. Card reading device 106 may accept an integrated circuit card (ICC) 234.

Fig. 3 depicts ICC 234 according to one embodiment of the present invention. Various mechanical and electrical characteristics of ICC 234 and aspects of its interaction with card reading device 106 are defined by the following specifications, all of which are herein incorporated by reference.

Visa Integrated Circuit Card Specification, (Visa International Service Association 1996).

EMV Integrated Circuit Card Specification for Payment Systems, (Visa International Service Association 1996).

EMV Integrated Circuit Card Terminal Specification for Payment Systems, (Visa International Service Association 1996).

EMV Integrated Circuit Card Application Specification for Payment Systems, (Visa International Service Association 1996).

International Standard: Identification Cards -- Integrated Circuit(s) Cards with Contacts, Parts 1-6 (International Standards Organization 1987-1995).

Besides the electronic commerce features discussed in the present application, ICC 234 may provide the functionality of a credit card, debit card, ATM card, stored value card, identification card, etc. ICC 234 includes electrical contacts 302 for receiving power and exchanging information with card reading device 106. A magnetic stripe 304 allows storage of information for reading by magnetic stripe readers. An integrated circuit 306 includes a processor and memory for storing application information. An embossing area 308 is available for imprinting the cardholder name, account number, and expiration date.

The combination of memory and processor preferably implements a symmetric cryptographic processor and in certain embodiments an asymmetric cryptographic processor. The symmetric cryptographic processor preferably uses the DES algorithm to encrypt an externally generated value employing a symmetric key. The asymmetric cryptographic processor preferably uses the RSA algorithm to encrypt an

externally generated value employing a private asymmetric key. The symmetric key and asymmetric key are preferably stored in memory so as to be inaccessible to external devices interacting with integrated circuit card 234.

The use of SET ensures the integrity and authenticity of cardholder account data transmitted through the Internet and does not require the use of an ICC or any physical payment card to initiate a purchase transaction. SET defines the transmission of a digital signature from CAD 102 to merchant server 104 and payment gateway 108 to ensure that the data transmitted from the cardholder has not been changed. According to the present invention, this digital signature operation may be performed either by CAD 102 or by ICC 234. In conjunction with the digital signatures, the SET protocol allows the transmission of a certificate chain to the merchant, validating a relationship between the cardholder and issuer. According to the present invention, this certificate chain, if used, may be stored either on CAD 102 or on ICC 234.

According to SET, cardholder certificates function as electronic representation of a payment card. Each cardholder certificate is digitally signed by a financial institution using the private key of the financial institution. Thus the cardholder certificate can only be generated by a financial institution and cannot be altered by a third party. The cardholder certificate includes the public signature key of the cardholder, and a hash of the cardholder's account information and secret value known to the SET software operating on CAD 102. All of this data is signed with the private signature key of the financial institution. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. SET does not mandate the use of cardholder certificates but allows for their use to enhance security.

The cardholder certificate is verifiable through a hierarchy of trust. The cardholder certificate is linked to a signature certificate of the entity, a cardholder certificate authority (CCA), that digitally signed the cardholder certificate. The signature certificate of the CCA includes the public signature key of the CCA signed by geopolitical certificate authority (GCA) with its own private signature key. The CCA certificate is linked to a GCA certificate which includes the public signature key of the GCA signed by the payment brand (e.g., Visa, MasterCard, etc.) with its private signature key. The GCA certificate is linked to a payment brand certificate that includes the public signature key of the payment brand as signed by a root authority with its

private signature key. The payment brand certificate is in turn linked to a root authority certificate which includes the root's public signature key signed by the root's private key.

For each payment brand, there may be a GCA for each country. A recipient of the cardholder certificate will be able to verify it using the public signature key of the CCA. The public signature key of the CCA is verifiable by use of the public signature key of the GCA to decrypt the CCA certificate. In turn, the public signature key of the GCA is verifiable by using the payment brand public key to decrypt the GCA certificate. The payment brand public signature key is verifiable by using the root public signature key to decrypt the payment brand certificate. Thus, a merchant may verify a cardholder by traversing the certificate chain. SET provides for the certificate chain to be maintained on CAD 102. According to the present invention, the certificate chain may also be stored on ICC 234.

In one embodiment, the present invention augments the protections provided by SET using on-line authorization by issuer 112. Integrated circuit card 234 generates an authorization request cryptogram (ARQC) which is used by issuer 112 to authenticate the card.

The discussion that follows refers to three exemplary embodiments. In a first embodiment referred to as "Option 1," integrated circuit card 234 incorporates asymmetric cryptographic processing and stores a cardholder certificate and the chain of certificates leading from the cardholder certificate to the root. In a second embodiment referred to as "Option 2," integrated circuit card 234 does not incorporate asymmetric cryptographic processing and does not store the cardholder certificate and the other certificates of the chain. In "Option 2," however, a cardholder certificate and certificate chain are associated with integrated circuit but stored on CAD 102 which is capable of asymmetric cryptographic processing. In a third embodiment referred to as "Option 3," integrated circuit card 234 does not incorporate asymmetric cryptographic processing and does not store the cardholder certificate and the other certificates of the chain. Also, there is no cardholder certificate associated with this card and stored by CAD 102.

Fig. 4 is a top-level flowchart describing steps of transaction processing according to one embodiment of the present invention. Prior to processing of the transaction, at step 402, the cardholder shops, e.g., by browsing through the merchant's website. CAD 102 may be equipped with an HTTP-compatible browser to facilitate viewing catalog information stored on merchant server 104. At step 404, after the user

has decided to purchase particular goods or services, he or she initiates a request, e.g., by selecting a link or screen button within the browser. Merchant server 104 receives the request and responds by sending CAD 102 a merchant certificate and a payment gateway certificate at step 406. The merchant certificate includes the public key-exchange key of the merchant. The payment gateway certificate includes the public key-exchange key of the payment gateway. These certificates are signed with the private keys of CCAs to which the merchant and payment gateway are assigned. At step 408, software on CAD 102 verifies the merchant and payment gateway certificates by traversing the certificate chain to the root key.

At step 410, CAD 102 checks for the presence of integrated circuit card 234 in card reading device 106. If integrated circuit card 234 is not present, further operation is in accordance with SET techniques at step 412. If integrated circuit card 234 is present, processing proceeds to step 414 where CAD 102 selects the particular application on integrated circuit card 234 that incorporates the features of the present invention. According to the various EMV Specifications and the VIS Specification, integrated circuit card 234 may support multiple applications. If integrated circuit card 234 operates according to the VIS specification, the selected application is preferably a credit/debit application and there need not be a separate application defined for networked electronic commerce.

At step 416, initial application processing functions are performed between CAD 102 and integrated circuit card 234. CAD 102 issues a command to integrated circuit card 234 to retrieve a list of files and records stored on the card and related to the selected application. This command also retrieves a list of functions supported by the selected application. This list will indicate whether integrated circuit card 234 supports cardholder verification.

At step 417, CAD 102 sends a purchase initialization request to merchant server 104 in accordance with SET. The purchase initialization request includes the brand of integrated circuit card 234, e.g., "Visa." In response, merchant server 104 sends a purchase initialization request response to CAD 102. The purchase initialization request response preferably includes a transaction identifier uniquely identifying the transaction among other data specified by SET.

At step 418, CAD 102 retrieves the listed files and records associated with the selected application from integrated circuit card 234. The retrieved information

includes the cardholder's personal account number (PAN) and expiration date. For Option 1 cards, CAD 102 reads the cardholder certificate and certificate chain from integrated circuit card 234. According to the present invention, integrated circuit card 234 may also store a URL identifying a network address of the payment brand. CAD 102 retrieves this URL and accesses the identified network address to retrieve and display images identifying the card issuer and payment brand.

At step 420, CAD 102 performs cardholder verification if this is supported by integrated circuit card 234. Included in the files and records retrieved at step 418 is a list of cardholder verification methods supported by the card. The preferred method of cardholder verification is offline PIN processing. If CAD 102 also supports offline PIN processing, the cardholder is prompted for entry of his or her PIN. CAD 102 sends the entered PIN as cleartext to integrated circuit card 234. Integrated circuit card 234 compares the entered PIN with a reference PIN and returns the results of the comparison to CAD 102. CAD 102 records whether offline PIN processing was performed, whether a PIN was actually entered, and the results of the comparison to the reference PIN.

Step 422 begins an on-line authorization procedure where issuer 112 may verify the authenticity of integrated circuit card 234. CAD 102 requests generation of an authorization request cryptogram (ARQC) if PIN entry was successful, or an application authorization cryptogram (AAC) if PIN entry was not successful. A request for an AAC is tantamount to declining the transaction. The request for an ARQC or AAC includes variable data particular to the transaction, preferably including an amount authorized by the merchant, a transaction currency code previously supplied by the merchant, transaction date, and an unpredictable number.

In response to the request for an ARQC, integrated circuit card 234 preferably performs various card risk management functions including checking for previous authentication failures, PIN entry results, and other risk factors. If an AAC has been requested by CAD 102 or any of the risk factors are present, integrated circuit card 234 returns an AAC to CAD 102. CAD 102 responds to the AAC by terminating the transaction. If an ARQC has been requested and integrated circuit card 234 previously successfully performed the PIN comparison, integrated circuit card 234 responds by returning an ARQC.

Both an ARQC and an AAC preferably include the variable data listed above encrypted with a symmetric key unique to integrated circuit card 234. In a

preferred embodiment, the encryption algorithm is DES. Ultimately, the ARQC is sent to issuer 112 for on-line authentication of the card. Receipt of an AAC by CAD 102 result in termination of the transaction.

The unpredictable number is formed by CAD 102 through the following process. The transaction identifier, which is preferably a 20 byte value is divided into five 4-byte blocks. The first (leftmost) block is exclusive-ORed with the second block. The result of this first exclusive OR operation is exclusive-ORed with the third block. The result of the second exclusive OR operation is exclusive-ORed with the fourth block. The result of the third exclusive OR operation is exclusive-ORed with the fifth (rightmost) block to form the unpredictable number.

How CAD 102 formulates a purchase request to the merchant will depend on whether this is an Option 1, Option 2, or Option 3 system. At step 424, CAD 102 checks whether SET-related data including the cardholder certificate chain and a value known as the PAN secret are stored on integrated circuit card 234 indicating that the card is configured for Option 1. The PAN secret is the result of exclusive-ORing an arbitrary number associated with the card with an arbitrary number associated with the issuer. If the card is configured for Option 1, formulation of the purchase request occurs at step 426.

If the card is not configured for Option 1, CAD 102 checks at step 428 to see if it has the cardholder certificate chain and PAN secret internally stored, indicating an Option 2 system. If this is an Option 2 system, the purchase request is formulated at step 430. If the cardholder certificate chain and PAN secret are present on neither integrated circuit card 234 nor CAD 102, this indicates an Option 3 system and the purchase request is formulated at step 432.

According to SET, a purchase request includes two parts, order information (OI) and payment instructions (PI). The OI identifies the order to the merchant. The PI is not reviewed by the merchant but is instead forwarded to payment gateway 108. When a cardholder certificate is available, SET provides for generation of a dual signature for the OI and PI. Message digests for both the OI and PI are generated and concatenated. The message digest of the concatenation result is generated and encrypted using the cardholder private signature key to form a dual signature. The PI is encrypted with a randomly generated symmetric key. This randomly generated symmetric key along with the cardholder's account information is encrypted with the

private key-exchange key of the payment gateway. The purchase request as sent to the merchant includes the encrypted PI and OI. The purchase request also includes the cardholder certificate chain.

In the case of Option 1 processing at step 426, CAD 102 creates the PI and OI as defined by the SET Specification. Where the personal account number and expiration date would normally appear in the PI, CAD 102 includes a series of zeroes. CAD 102 forms a special data object including certain integrated circuit card-related data. This data includes the ARQC and the cleartext data encrypted within the ARQC including the unpredictable number. This special data object is embedded in the PI. All of the steps of generating the purchase request are performed by CAD 102 except for encrypting the message digest of the concatenation result using the cardholder private key. This step is performed by integrated circuit card 234. In a preferred embodiment where integrated circuit card 234 conforms to the VIS specification, this encryption is performed using the INTERNAL AUTHENTICATE command included in the specification.

Option 2 processing at step 430 is the same as Option 1 processing at step 426, except that all steps of forming the purchase request are now performed by CAD 102 including encrypting the message digest of the concatenation result using the cardholder private key.

In the case of Option 3 processing at step 432, CAD 102 creates the PI and OI as defined by the SET specification. As with Option 1 and Option 3, the integrated circuit card-related data is included with the PI. However, no dual signature is created for the payment request.

At step 434, CAD 102 sends the purchase request to merchant server 104. At this time, integrated circuit card 234 is no longer needed to complete the transaction and CAD 102 may prompt the cardholder to remove his or her card from card reading device 106.

At step 436, merchant server 104 processes the purchase request in accordance with SET. A portion of the purchase request is the PI which is forwarded to payment gateway 108.

At step 438, payment gateway 108 processes the PI. Payment gateway 108 decrypts the PI using its private key-exchange key. After decrypting the PI, payment gateway 108 checks for the card-related data in the PI to determine if the

purchase request involved use of an integrated circuit card. Once this has been verified, payment gateway 108 recalculates the unpredictable number from the transaction identifier and the merchant identifier it obtains from the ARQC. The result is compared with the unpredictable number transmitted within the PI. If there is no match, the transaction is rejected. The PAN and card expiration date are decrypted.

Payment gateway 108 sends issuer 112 via acquirer server 109 an authorization request that includes the data related to the payment transaction. The authorization request also preferably includes information indicating whether or not SET certificates were used and whether these certificates were present on integrated circuit card 234. Issuer 112 is aware of the unique symmetric key of the cardholder and attempts to verify the ARQC from the cleartext information included in the integrated circuit card related data. Issuer 112 applies the unique cardholder key to symmetrically encrypt the cleartext information and obtain ARQC'. If ARQC' matches ARQC, issuer 112 sends an authorization response message to payment gateway 108 indicating that the transaction is authorized by issuer 112. Payment gateway 108 responds to receipt of this authorization request message by sending an authorization message to merchant server 104. Merchant server 104 may then fulfill the order.

The card authentication operation of user 118 provides security that enhances or substitutes for the protection offered by the SET cardholder certificate. This security is potentially available to the cardholder through multiple acceptance devices, offering portability unavailable with prior art networked electronic commerce technologies.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereunto without departing from the broader spirit and scope of the invention as set forth in the appended claims and their full scope of equivalents. For example, the specification has discussed enhancements to the EMV, VIS, and SET specifications. The present invention is not, however, limited to use with any particular protocol or specification for cards electronic commerce.

WHAT IS CLAIMED IS:

1. A computer-implemented method for processing transactions over a network comprising the steps of:

establishing a connection between a card access device coupled to said network and an integrated circuit card;

transferring a cryptogram generation command comprising challenge data from said card access device to said integrated circuit card;

in response to said cryptogram generation command, using said integrated circuit card to encrypt said challenge data to form a response;

transferring said response from said integrated circuit card to said card access device;

forming a payment instruction message at said card access device, said payment instruction message comprising said response; and

encrypting at least a portion of said payment instruction message using asymmetric cryptographic techniques.

2. The method of claim 1 further comprising the step of sending said encrypted payment instruction message from said card access device to a merchant via said network.

3. The method of claim 1 wherein said step of encrypting said payment instruction message comprises using a symmetric key to encrypt said at least a portion of said payment instruction message and encrypting said symmetric key with a public key of a payment processor.

4. The method of claim 1 further comprising the steps of:

forming an order information message at said card access device;

hashing said order information message to obtain a digest of said order information message;

hashing said payment instruction message to obtain a digest of said payment instruction message;

concatenating said digest of said order information message and said digest of said payment instruction message to obtain a concatenated digest; and

encrypting said concatenated digest with a private signature key particular to said integrated circuit card to obtain a signed concatenated digest.

5. The method of claim 4 wherein said encrypting said concatenated digest step is performed by said integrated circuit card.

6. The method of claim 4 wherein said encrypting said concatenated digest step is performed by said card access device.

7. The method of claim 1 wherein said challenge comprises an unpredictable number.

8. The method of claim 1 wherein said unpredictable number is derived from an identifier identifying a particular merchant and an identifier identifying a particular transaction.

9. A computer program product for use with a computer coupled to a network and a card reading device facilitating secure electronic commerce, said computer program product comprising:

code for establishing a connection between said computer and an integrated circuit card in communication with said card reading device;

code for transferring a cryptogram generation command comprising challenge data from said computer to said integrated circuit card;

code for receiving a response to said cryptogram generation command from said integrated circuit card;

code for forming a payment instruction message, said purchase instruction message comprising said response; and

a computer-readable medium for storing the codes.

10. The computer program product of claim 9 further comprising code for encrypting said payment instruction message using asymmetric cryptographic techniques.

11. The computer program product of claim 10 further comprising the step of sending said encrypted payment instruction message from said card access device to a merchant via said network.

12. The computer program product of claim 10 wherein said code for encrypting said payment instruction message comprises code for using a symmetric key to encrypt said payment instruction message and encrypting said symmetric key with a public key of a payment processor.

13. The computer program product of claim 9 further comprising:

code for forming an order information message at said card access device;

code for hashing said order information message to obtain a digest of said order information message;

code for hashing said payment instruction message to obtain a digest of said payment instruction message;

code for concatenating said digest of said order information message and said digest of said payment instruction message to obtain a concatenated digest; and

code for encrypting said concatenated digest with a secret signature key particular to said integrated circuit card to obtain a signed concatenated digest.

14. An integrated circuit card comprising:

an interface for receiving external commands and data;

a symmetric cryptographic processor that encrypts a challenge value received via said interface to form a response to transmit via said interface;

an asymmetric cryptographic processor that encrypts a value received from said interface using a private key unique to said integrated circuit card; and

a memory storing said key and a certificate comprising a public key matching said private key unique to said integrated circuit card, said public key being signed by a private key of a certificate authority.

15. The integrated circuit card of claim 14 wherein said key is inaccessible to said interface.

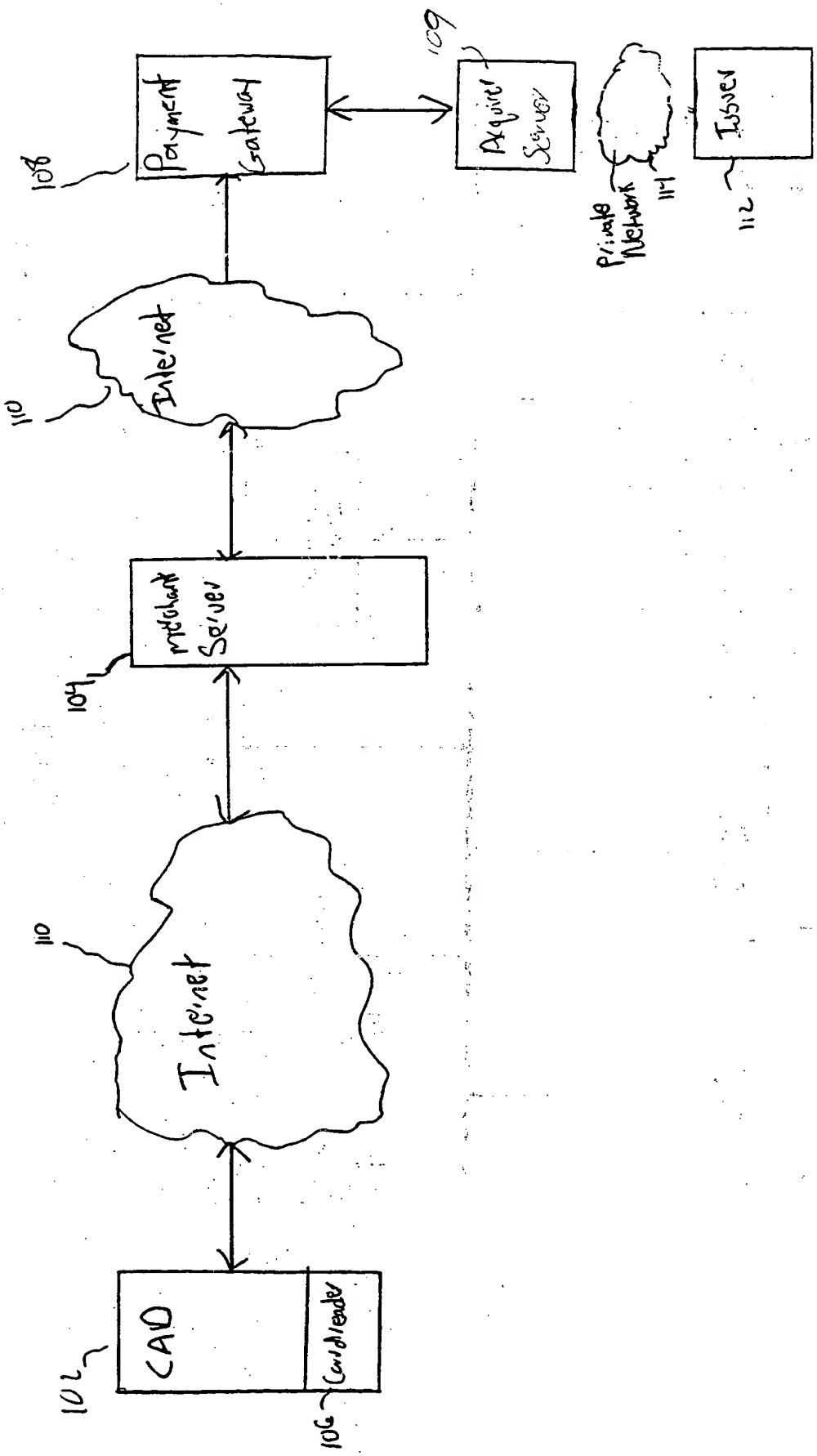


Fig. 1

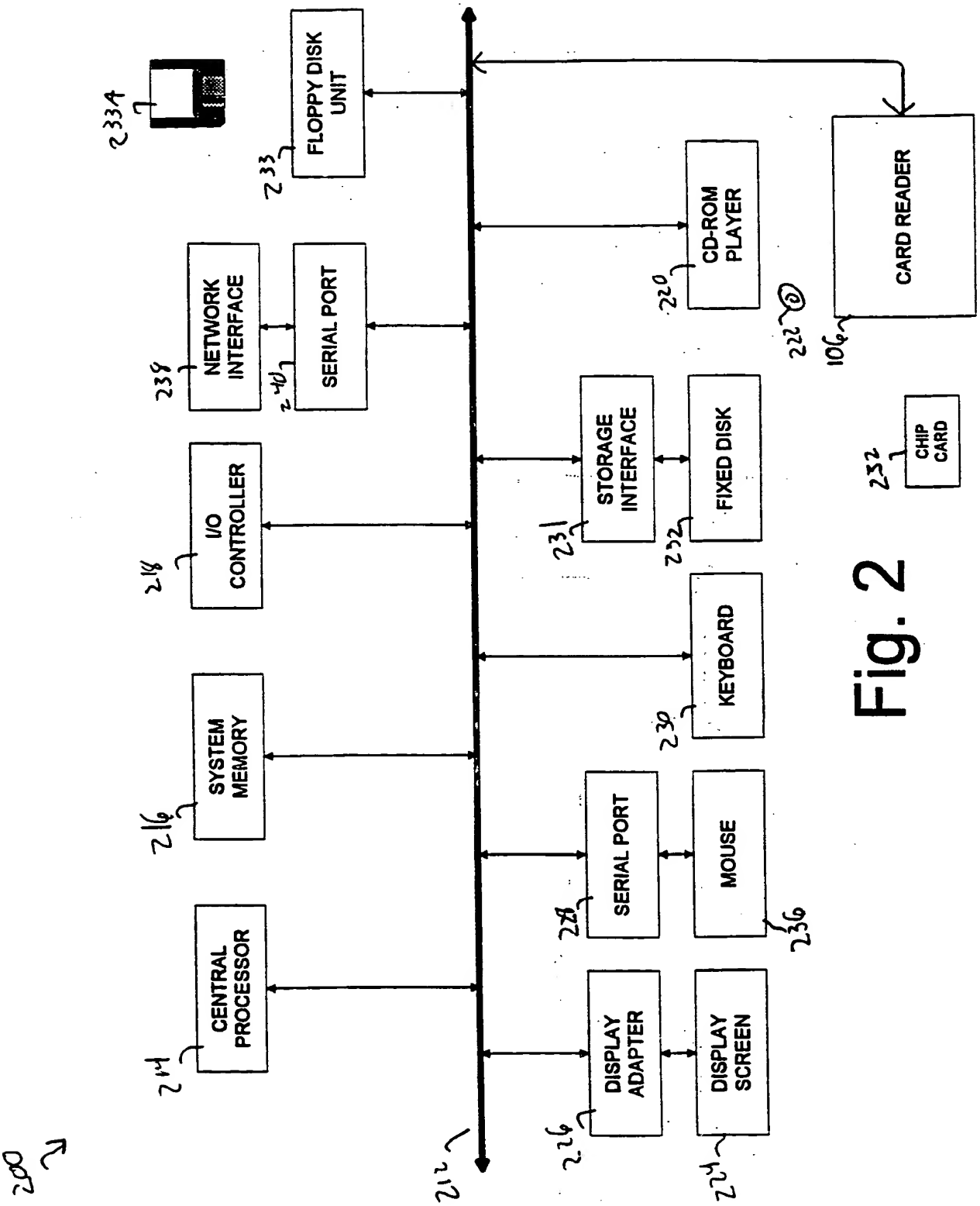


Fig. 2

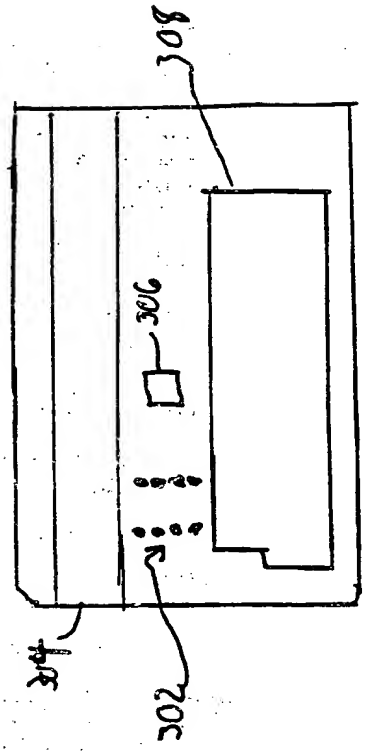


Fig. 3

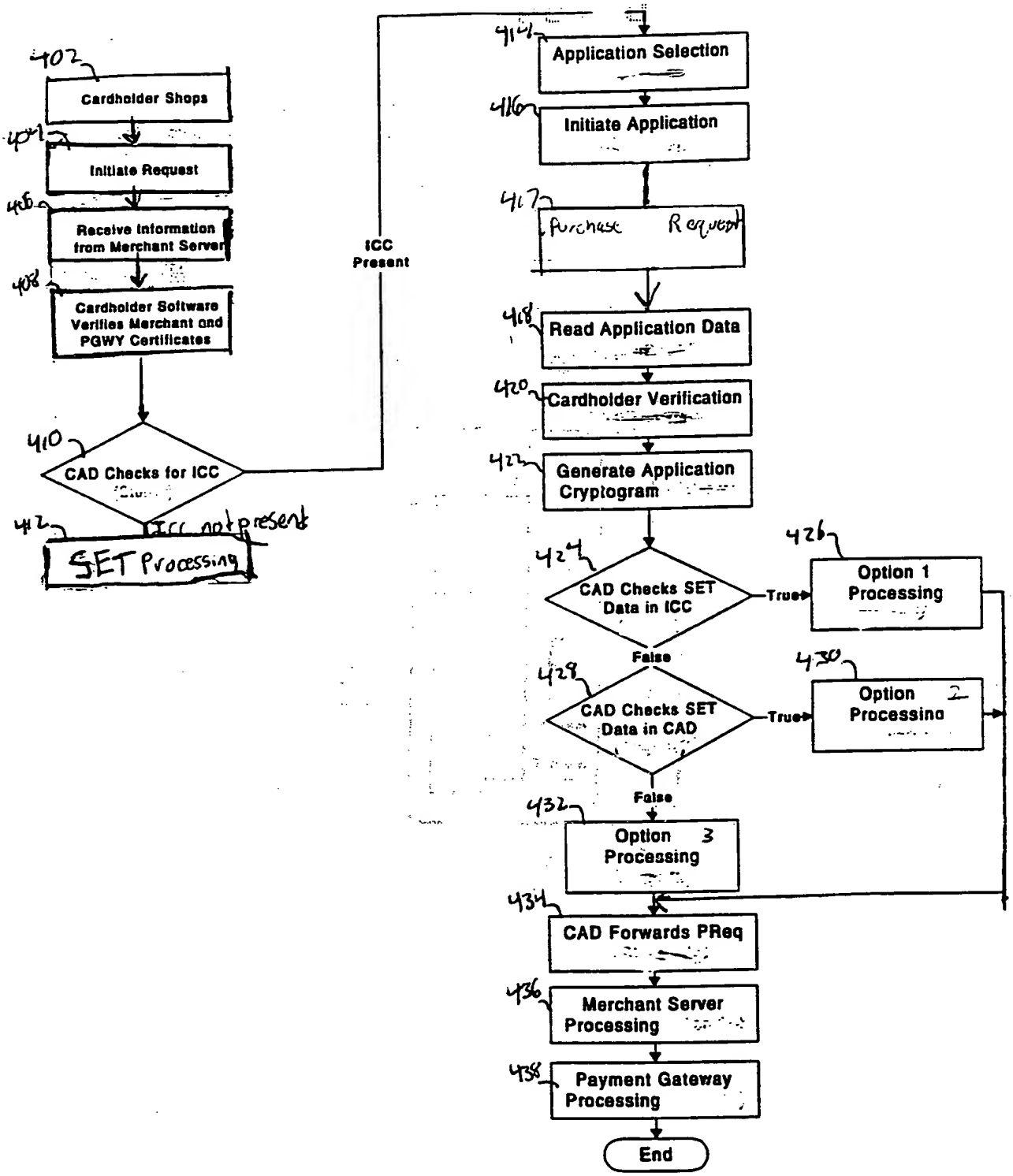


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/04606

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04K 1/00; H04L 9/00
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 49, 23, 24, 21, 28, 29, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 5,754,656 A (NISHIOKA, et al.) 19 May 1998 (19/05/98).	1-15
A, P	US 5,742,756 A (DILLAWAY, et al.) 21 April, 1998 (21/04/98).	1-15
A, P	US 5,721,781 A (DEO, et al.) 24 February 1998 (24/02/98).	1-15
A, P	US 5,706,349 (ADITHAM, et al.)06 January 1998 (06/01/98).	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 JUNE 1998	Date of mailing of the international search report 08 JUL 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Diane Smith for DAVID CAIN Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/04606

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

380/25, 49